eCitadel Practice Round

Linux Mint 21

Answer Key

Welcome to the eCitadel Practice Round! This document will provide you with information on how to solve the vulnerabilities on a Linux Mint 21 operating system. The goal of the practice round is to give beginners a chance to familiarize themselves with the competition structure.

The vulnerabilities in this image are some of the most basic ones found during an eCitadel competition. Even if you do very well with these vulnerabilities, you will experience greater difficulty with the actual competition.

Below are the answers to the problems that are being scored in this image. Each one includes information on how the problem was found (if applicable), how it was solved, and why it is important from a cybersecurity standpoint.

It is also possible to lose points during the competition. Simple penalties that may arise are noted below the answers. There are many ways to solve some of the problems below. This answer key just shows one method in each case.

Answers

1) Forensics Question 1 Correct: 10 pts.

- How do I find this problem?

  When you open an image, please read all the "Forensics Questions" thoroughly before modifying the image as you may change something that prevents you from answering the question correctly. There is a file on the Desktop here named "Forensics Question 1".

- How do I solve this problem?

  This question asks for the first table listed when you run "SHOW TABLES" on the "wordpress" database.

  Open a terminal and type **sudo mysql -u root -p** . The password for the SQL database can be found in the README. Switch to the wordpress database with **USE wordpress;** and then run **SHOW TABLES;** . Exit mysql by typing **quit** .

  The answer to this problem is the first table listed in the tables view.

- Why is fixing this problem important?

  When managing a database, it's important to know common SQL queries.

2) Forensics Question 2 Correct: 10 pts.

- How do I find this problem?

  When you open an image, please read all the "Forensics Questions" thoroughly before modifying the image as you may change something that prevents you from answering the question correctly. There is a file on the Desktop here named "Forensics Question 2".

- How do I solve this problem?

  This question asks you to find the absolute path of the directory containing prohibited MP3 files.

  In a terminal type locate '*.mp3'. In the output of locate you can see the file system location of files with the extension .mp3. The mp3 files under cyan's Music directory appear to be nonwork related.

  The answer to this question is the absolute path to the mp3 files starting with the root directory /.

- Why is fixing this problem important?

  Knowing how to efficiently find files of different types on a Linux operating system will help you quickly identify many different types of security issues such as prohibited files and software, sensitive information, backdoors, services, and important configuration files.

3) Removed unauthorized users maroon and rose: 4 pts each for a total of 8.

- How do I find this problem?

One of the first things you should do when starting an image during a competition is check the README file on the desktop. The authorized administrators and users listed in the README are the only users that should exist on the system (aside from legitimate built-in system accounts and those used for services). All unauthorized user accounts should be removed.

- How do I solve this problem?

  Click the **Show Applications** button on the bottom of the Launcher and open **Control Centre** then select **Users and Groups**. Select the users **maroon** and **rose**. Click on **Delete**. If prompted type the password of your current user account. The password for your current user account can be found in the README. Since this is a competition environment and a further analysis of these users' files is not necessary, click **Delete Files**.

  Why is fixing this problem important?

  Computer access should be limited to just those who need to use it to complete their tasks. By leaving unauthorized user accounts on the image, unauthorized individuals may be able to log on to the domain and make changes that could affect the safety and security of legitimate users. Unauthorized user accounts also give adversaries a greater attack surface.

4) A minimum password length is required: 5 pts.

- How do I find this problem?

  Enforcing industry recommended password policies is good cybersecurity practice.

- How do I solve this problem?
  In a terminal, open the **/etc/pam.d/common-password** file with administrator privileges. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README. Find the line with the **pam_unix.so** module, and at the end of the line, add **minlen=10** . Save the file.

- Why is fixing this problem important?
  Setting a minimum password length prevents users from setting short passwords that are insecure.

5) IPv4 forwarding has been disabled: 5 pts.

- How do I find this problem?

  Setting secure Linux kernel parameters is a good cybersecurity practice.

- How do I solve this problem?

  In a terminal, open the **/etc/sysctl.conf** file with administrator privileges. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README. Find the line that says **net.ipv4.ip_forward=1** and change the value to **0**. Save the file, then run **sysctl -p** to reload the settings.

- Why is fixing this problem important?

This Linux server is not acting as a router, so we do not need to be forwarding packets meant for other destinations (other than ourself).

6) Uncomplicated Firewall (UFW) protection has been enabled: 8 pts.

- How do I find this problem?

  Enabling a host-based firewall is very important to system security. You can check the status of UFW by typing **sudo ufw status**. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- How do I solve this problem?

  In a terminal, type **sudo ufw enable**. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- Why is fixing this problem important?

  Enabling and properly configuring a firewall is critical to ensuring that you are only allowing known, authorized traffic in and out of your computer.

7) POP3 service has been disabled or removed: 6 pts.

- How do I find this problem?

  Stopping and disabling insecure or unnecessary services is an important principle of good cybersecurity. Many services need to be running to ensure normal and secure operation of computer systems. Reading about the services on your system and doing research can help you determine the importance of a service and if it is necessary for normal operation. Additionally, business critical services listed in the README should remain running at all times. Running services can be found by running the command **systemctl list-units --type=service --state=active** in a terminal.

- How do I solve this problem?

  In a terminal, type **sudo systemctl stop dovecot** to stop the service. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README. After stopping the service, type **sudo systemctl disable dovecot** to prevent it from starting automatically in the future.

- Why is fixing this problem important?

  Disabling unnecessary services can limit your attack surface. The less services an adversary has to attack and potentially exploit, the lower your risk. Adversaries may attack known or unknown vulnerabilities in services to obtain information, escalate privileges, or gain unauthorized access.

8) Install updates from important security updates: 6 pts.

- How do I find this problem?

  Updating your operating system is an important principle of good cybersecurity. Installing updates from security update sources ensures you are receiving the latest security updates.

- How do I solve this problem?

  In a terminal, open the file **/etc/apt/sources.list.d/official-package-repositories.list** with administrator privileges. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README. Uncomment the line beginning with **deb http://security.ubuntu.com/ubuntu/ jammy-security main** . Save the file.

- Why is fixing this problem important?

  Including security updates in your package sources ensures you are receiving the latest security updates whenever you run updates.

9) Systemd, MariaDB, and OpenSSH has been updated: 4 pts each for a total of 12.

- How do I find this problem?

  Updating installed applications and services to fix security vulnerabilities is an important principle of good cybersecurity.

- How do I solve this problem?

  Open a terminal and run **sudo apt update -y** to refresh your list of available packages from your update sources. Then run **sudo apt upgrade -y** to install the updates. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- Why is fixing this problem important?

  When security vulnerabilities are found in software, the software vendor publishes updates that patch the security vulnerabilities. Adversaries can more easily compromise your system if software is present that has known security vulnerabilities. Ensuring software is up to date removes known security vulnerabilities.

10) Prohibited MP3 files are removed: 6 pts.

- How do I find this problem?

  The README specifically states that non-work related media files are prohibited. There are several ways and commands that can be used to find files and file types including **locate, find, file**.

- How do I solve this problem?

  In a terminal type **locate ' *.mp3'**. In the output of locate you can see the file system location of files with the extension .mp3. The mp3 files under cyan's Music directory appear to be non-work related. Type **sudo rm /home/cyan/Music/*.mp3** If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- Why is fixing this problem important?

  In addition to being specifically prohibited in the README, media files can also be used to compromise media viewer/player software and could introduce unwanted legal and regulatory issues.

11) Prohibited software Game Conqueror and ManaPlus removed: 4 pts each for a total of 8.

- How do I find this problem?

  Removing unauthorized and potentially unwanted programs from a computer is an important cybersecurity principle. Third party software installed on the system should be limited to the software listed in the README, and software required for normal operation of the operating system, and services and software listed in the README. Auditing the list of currently installed packages on the system will show you that **Game Conqueror** and **ManaPlus** are installed.

- How do I solve this problem?

  In a terminal, type **sudo apt remove gameconqueror** and **sudo apt remove manaplus** and press **Enter**. Type **Yes** or **y** to remove the application.

- Why is fixing this problem important?

  Removing unauthorized software from your system is important for limiting you risk and reducing your attack surface. Unauthorized programs may leak confidential information, interfere with business-critical software and services, contain various malware, contain security vulnerabilities, or could introduce unwanted legal and regulatory issues.

12) Chromium blocks pop-ups and redirects: 8 pts.

- How do I find this problem?

  Chromium is listed as the primary browser in the README. As such, the security settings within the browser should be configured.

- How do I solve this problem?

  Open Google Chrome and navigate to "chrome://settings/content/popups". Select **Don't allow sites to send pop-ups or use redirects**.

- Why is fixing this problem important?

  Allowing pop-ups could lead to a user clicking on a malicious pop-up and lead to a future breach.

13) SSH does not permit empty passwords: 8 pts.

- How do I find this problem?

  OpenSSH Server is listed in the README as a critical service. It's important to research how to secure critical services without breaking the required functionality of the service.

- How do I solve this problem?

  In a terminal open **/etc/ssh/sshd_config** with administrator privileges. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

  Change the line that says **PermitEmptyPasswords yes** to **PermitEmptyPasswords no**. Save the file and exit. Then restart the service with **sudo systemctl restart sshd**

- Why is fixing this problem important?

  We should always require a password when logging into the SSH server, as an additional security measure.

Penalties

1) OpenSSH service has been stopped or removed: -5 pts.

- Why is this a penalty?
  The README states that OpenSSH is a critical service.

2) MariaDB service has been stopped or removed: -5 pts.

- Why is this a penalty?
  The README states that MariaDB is a critical service.

3) Chromium has been removed: -5 pts.

- Why is this a penalty?
  The README states that Chromium is required software.